Protego: A Low-Overhead Open-Source I/O Physical Memory Protection Unit for RISC-V

SSH-SoC 2023, July 9th, 2023

Integrated Systems Laboratory (ETH Zürich)

Nils Wistoff	nwistoff@iis.ee.ethz.ch
Andreas Kuster	mail@andreaskuster.ch
Michael Rogenmoser	michaero@iis.ee.ethz.ch
Robert Balas	balasr@iis.ee.ethz.ch
Moritz Schneider	moritz.schneider@inf.ethz.ch
Luca Benini	lbenini@iis.ee.ethz.ch

PULP Platform

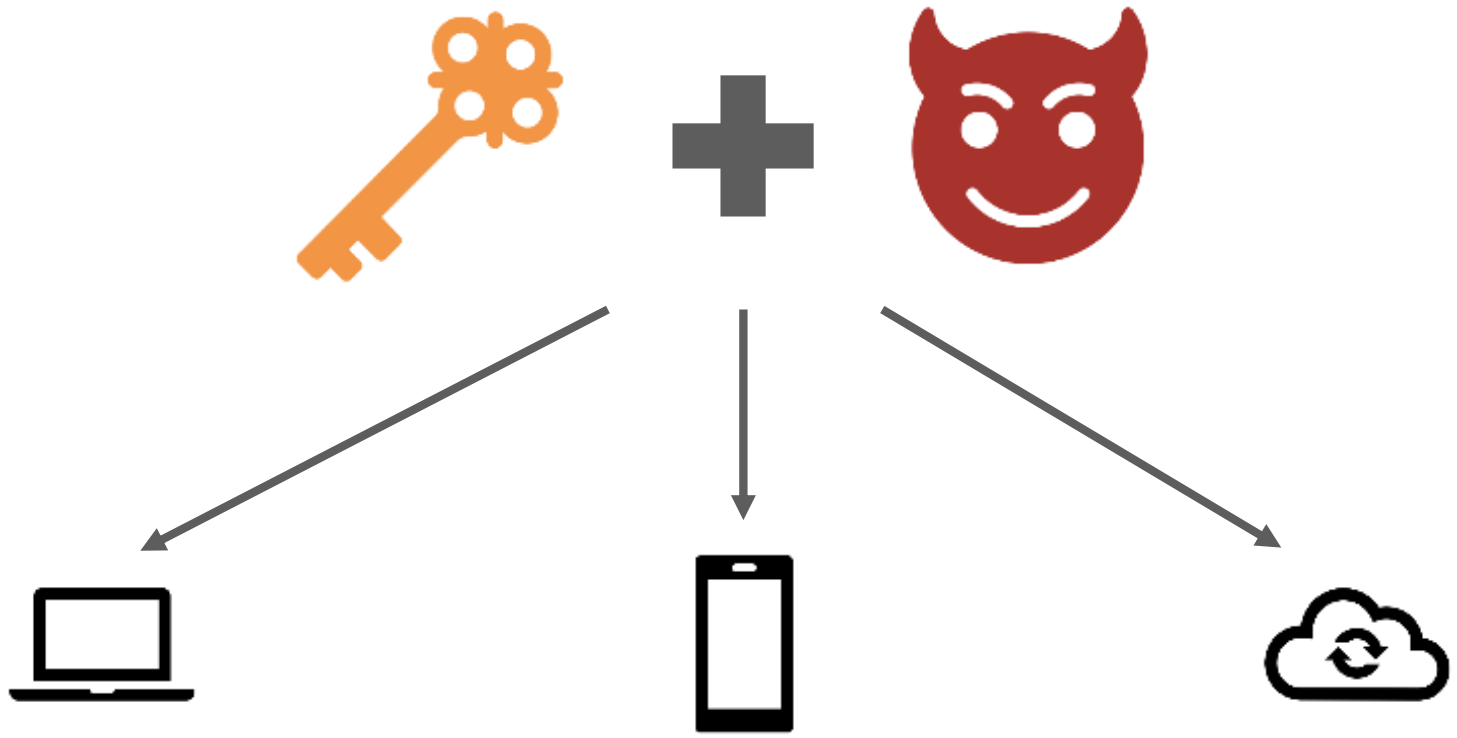
Open Source Hardware, the way it should be!

@pulp_platform

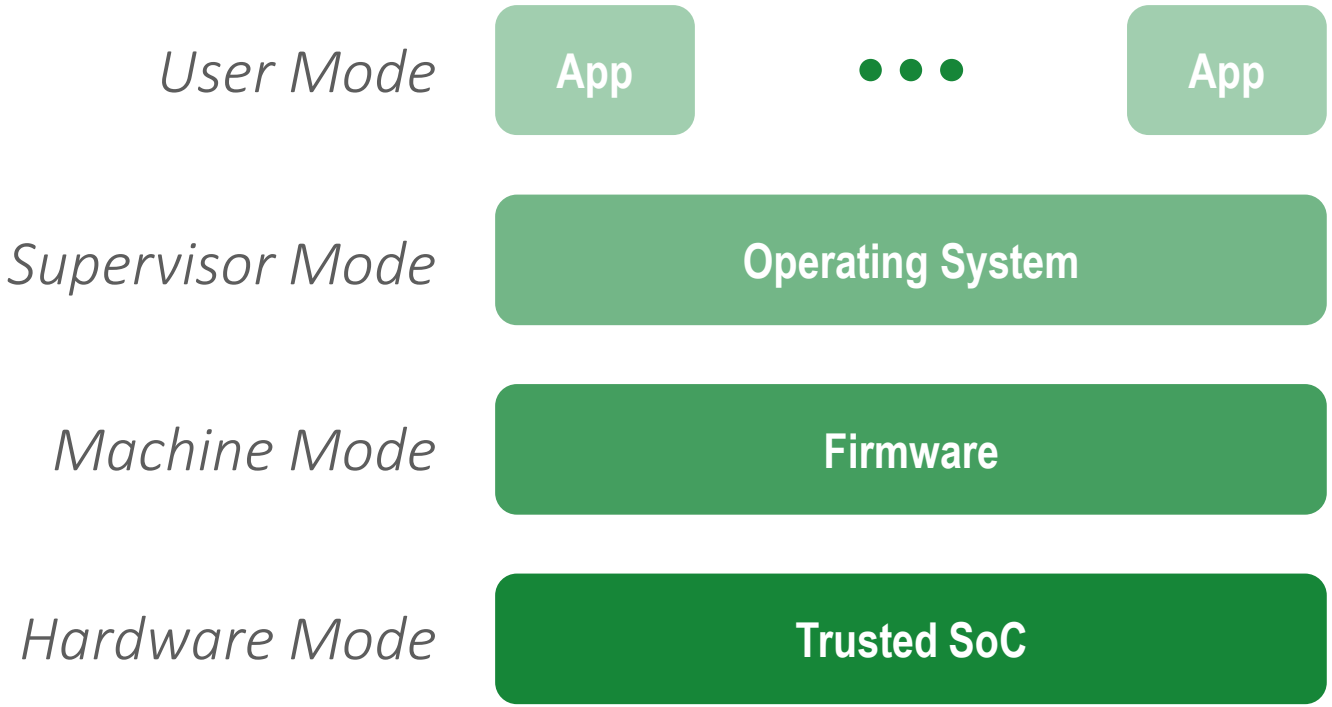
pulp-platform.org

youtube.com/pulp_platform

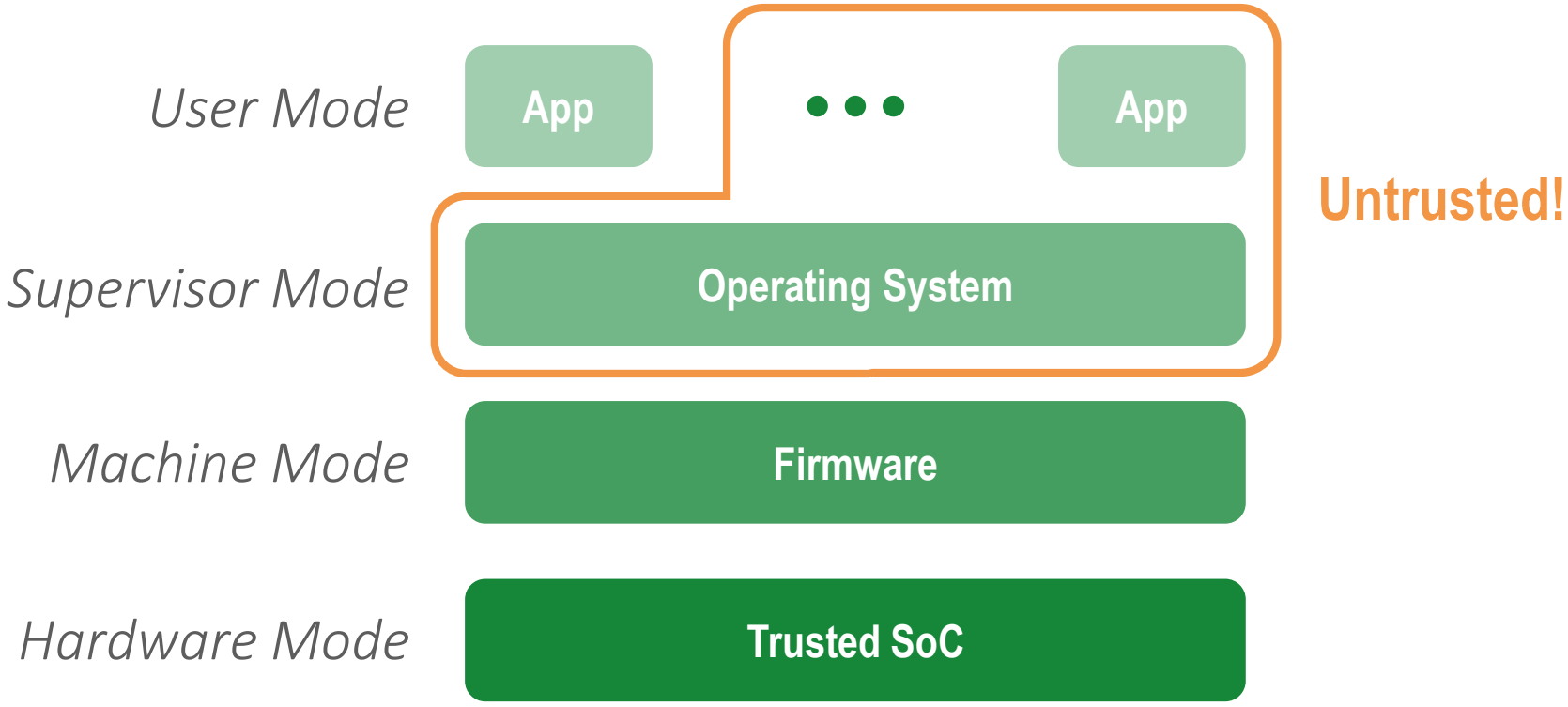
Hardware shared by sensitive & untrusted workloads



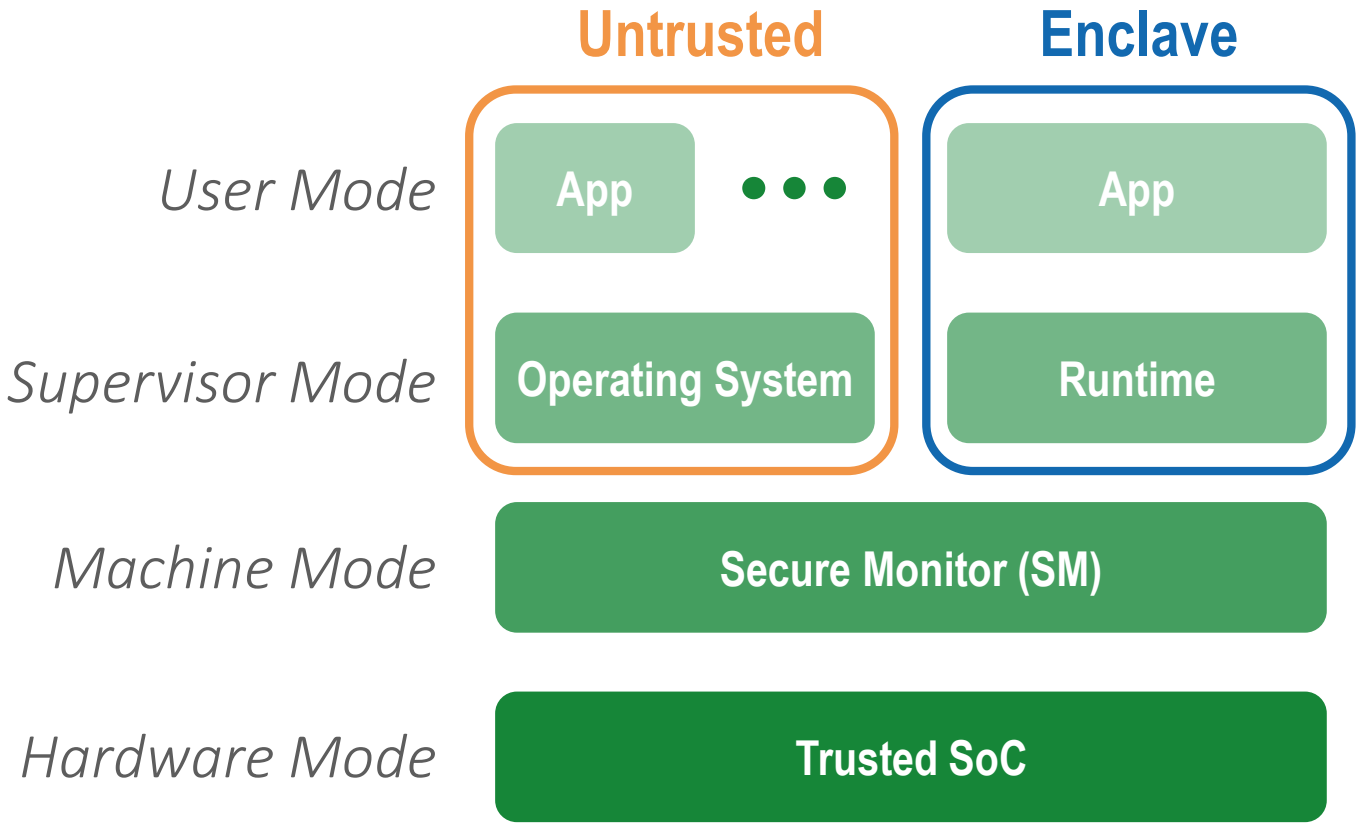
Threat Model



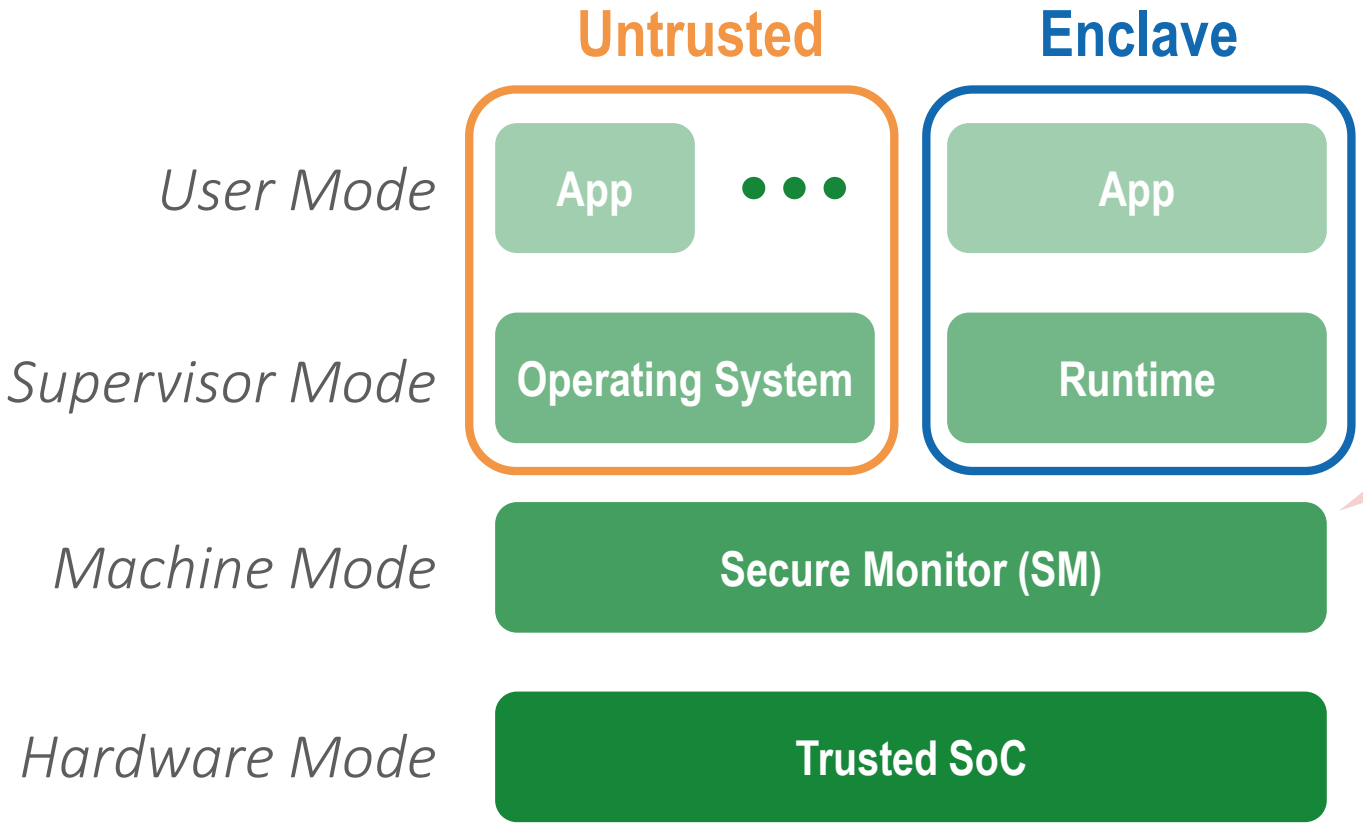
Threat Model



Threat Model



Threat Model

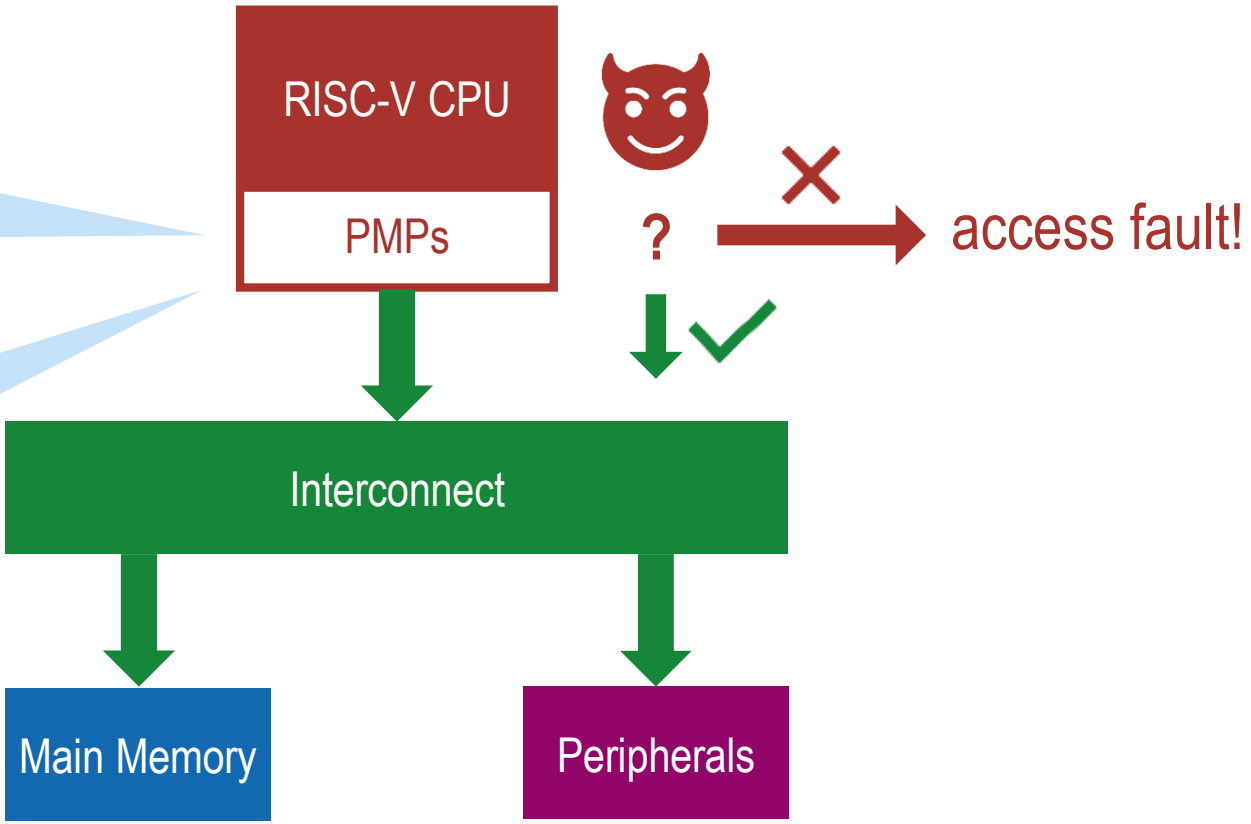


Isolation using **Physical Memory Protection (PMP)**

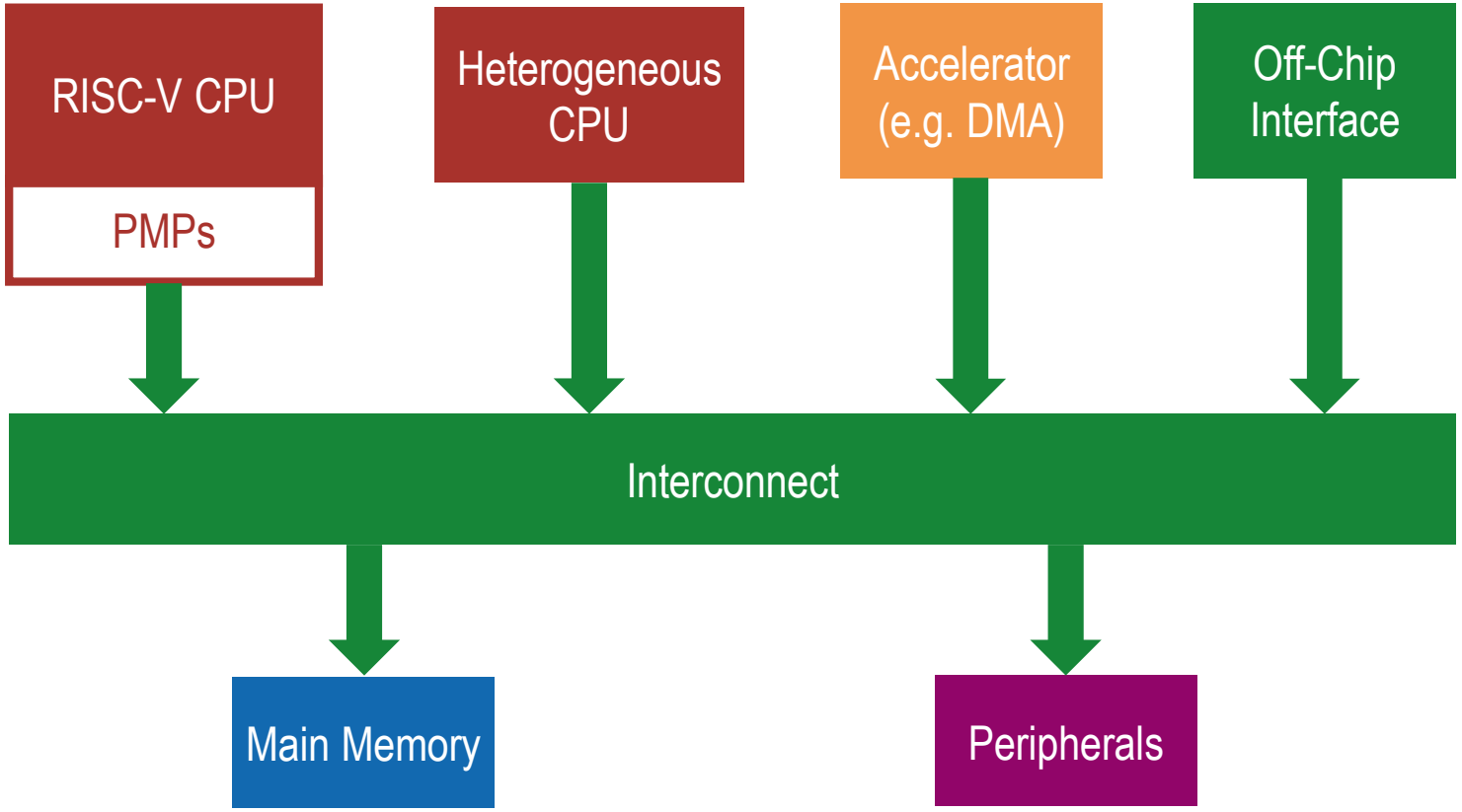
Physical Memory Protection (PMP)

Set of **control and status registers (CSRs)** define permitted memory ranges

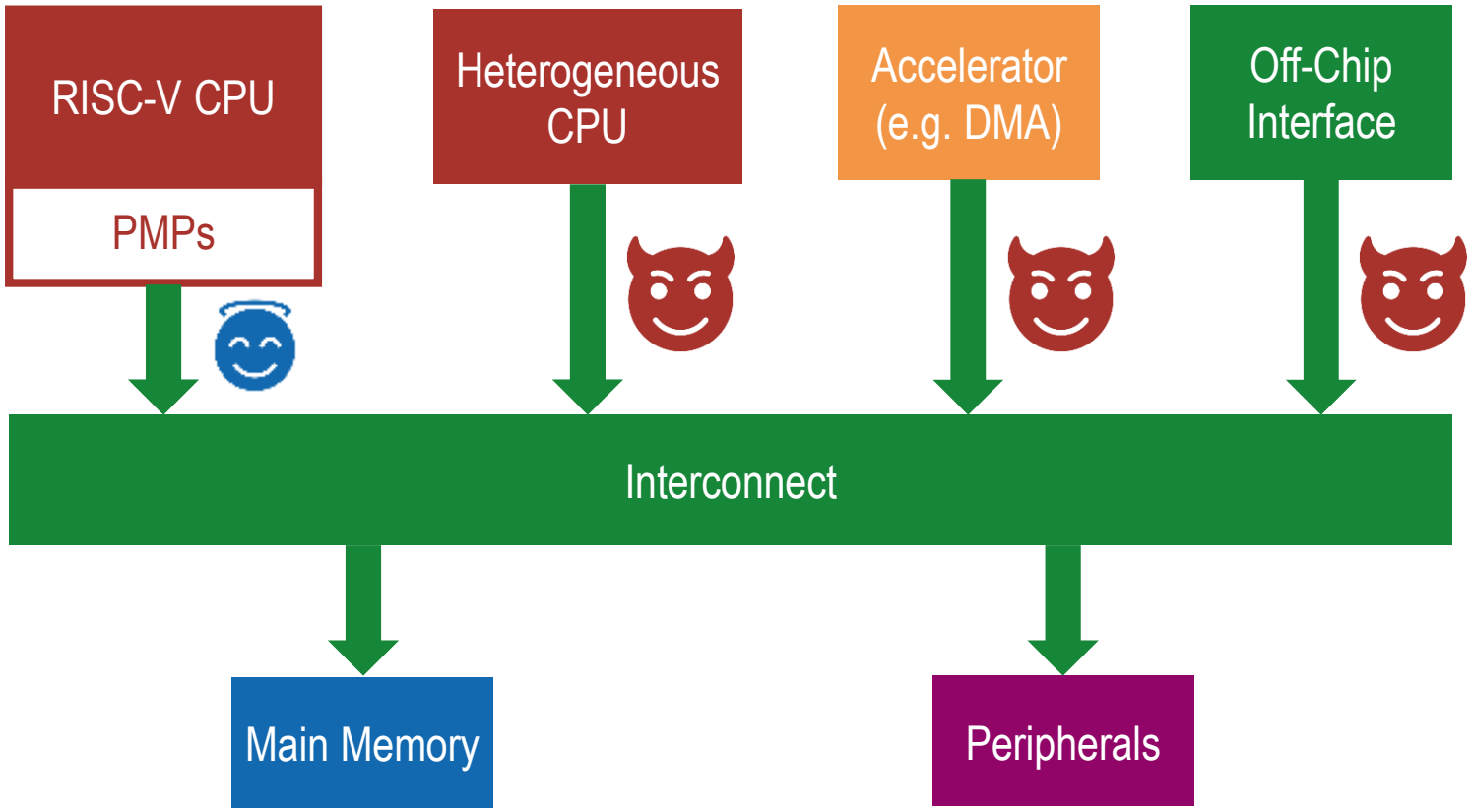
Check each memory access against PMP configuration



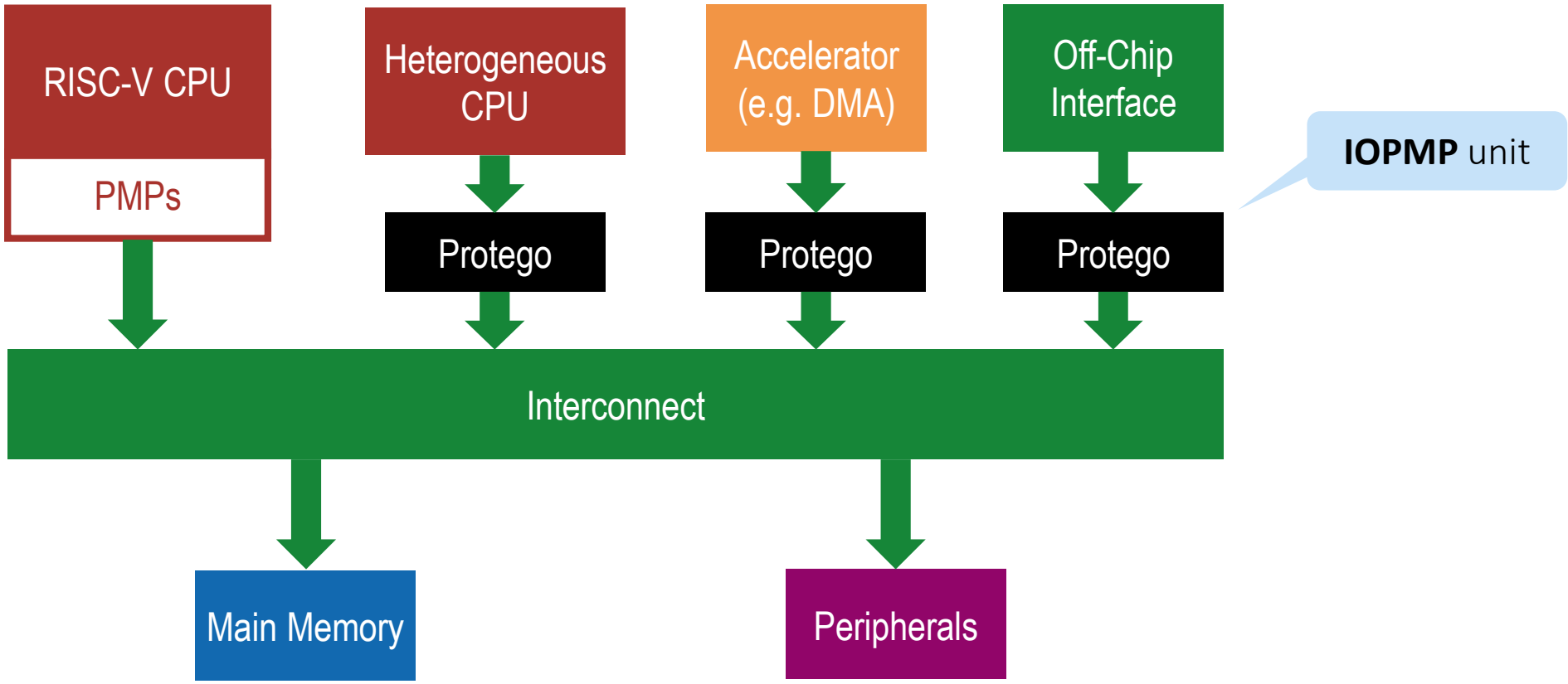
PMP in Heterogeneous Systems



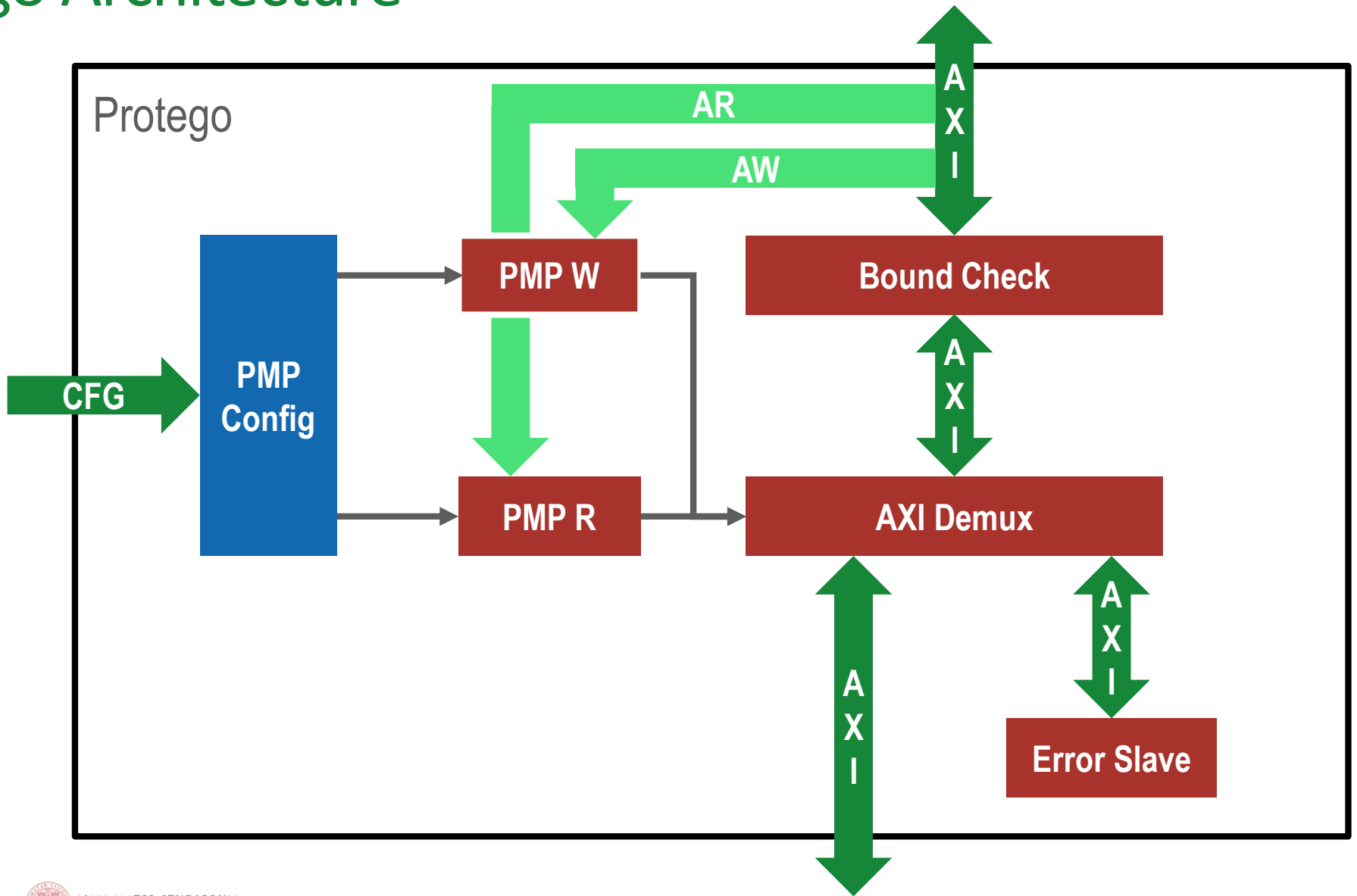
PMP in Heterogeneous Systems



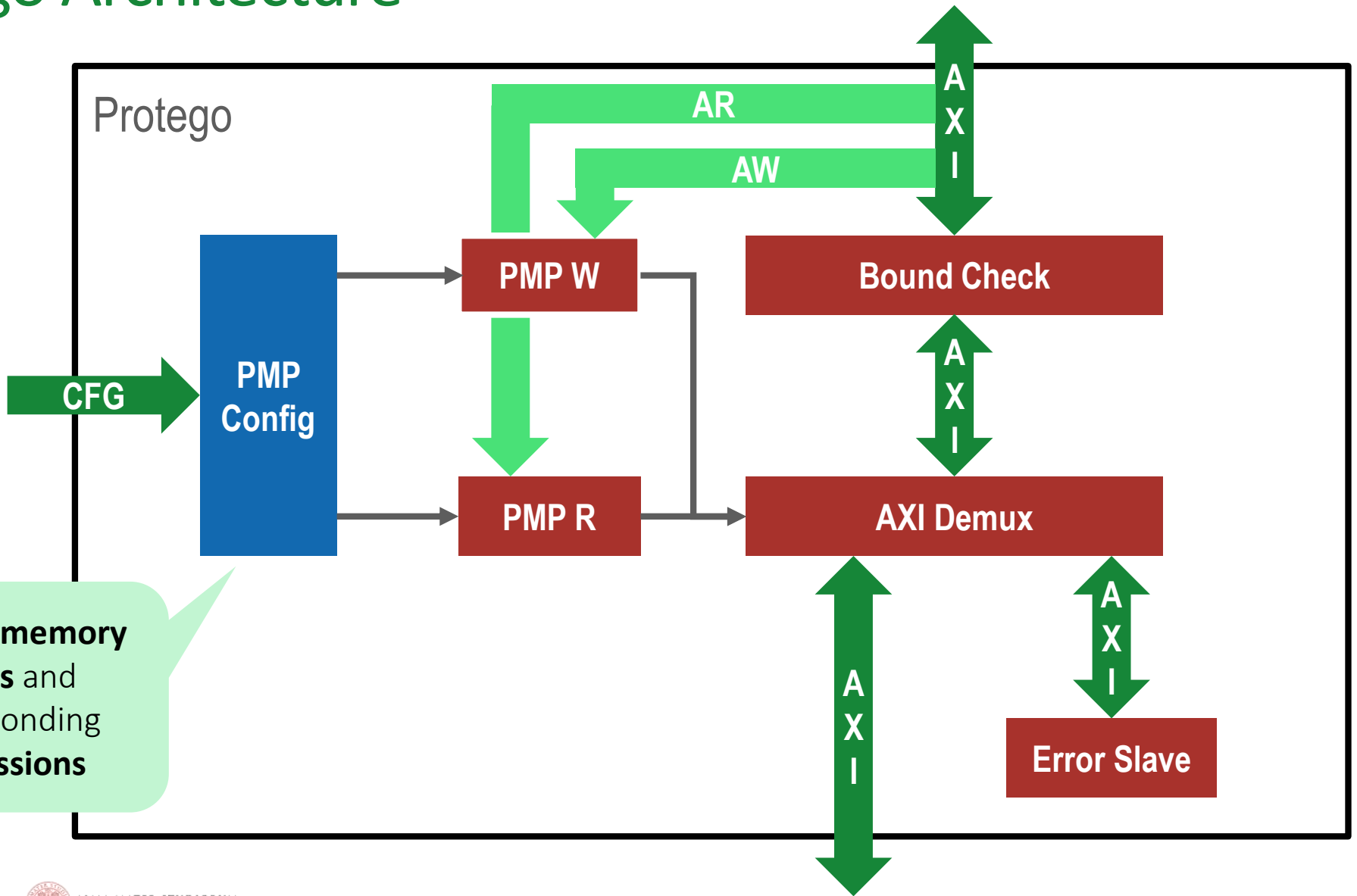
I/O Pysical Memory Protection (IOPMP)



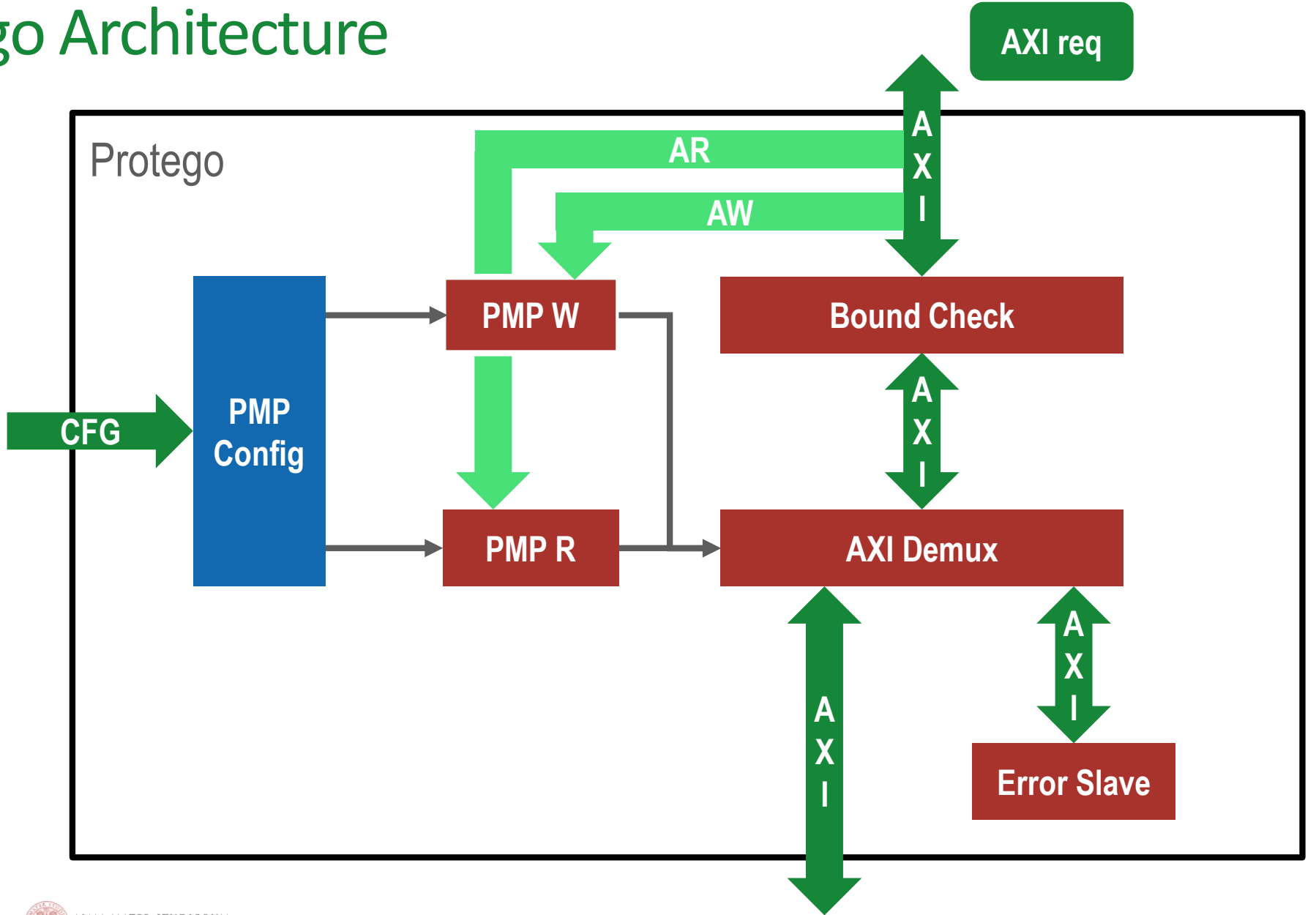
Protego Architecture



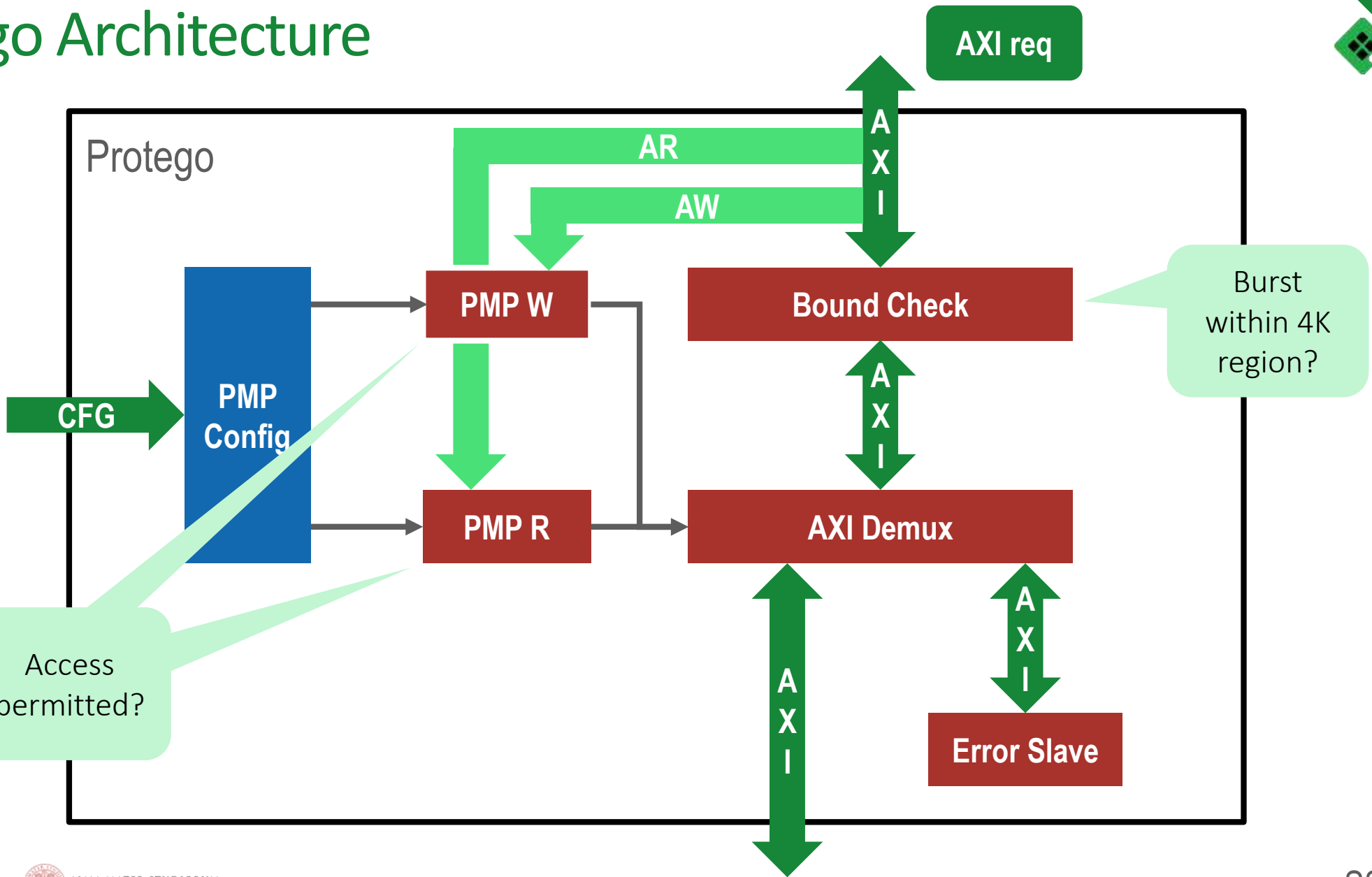
Protego Architecture



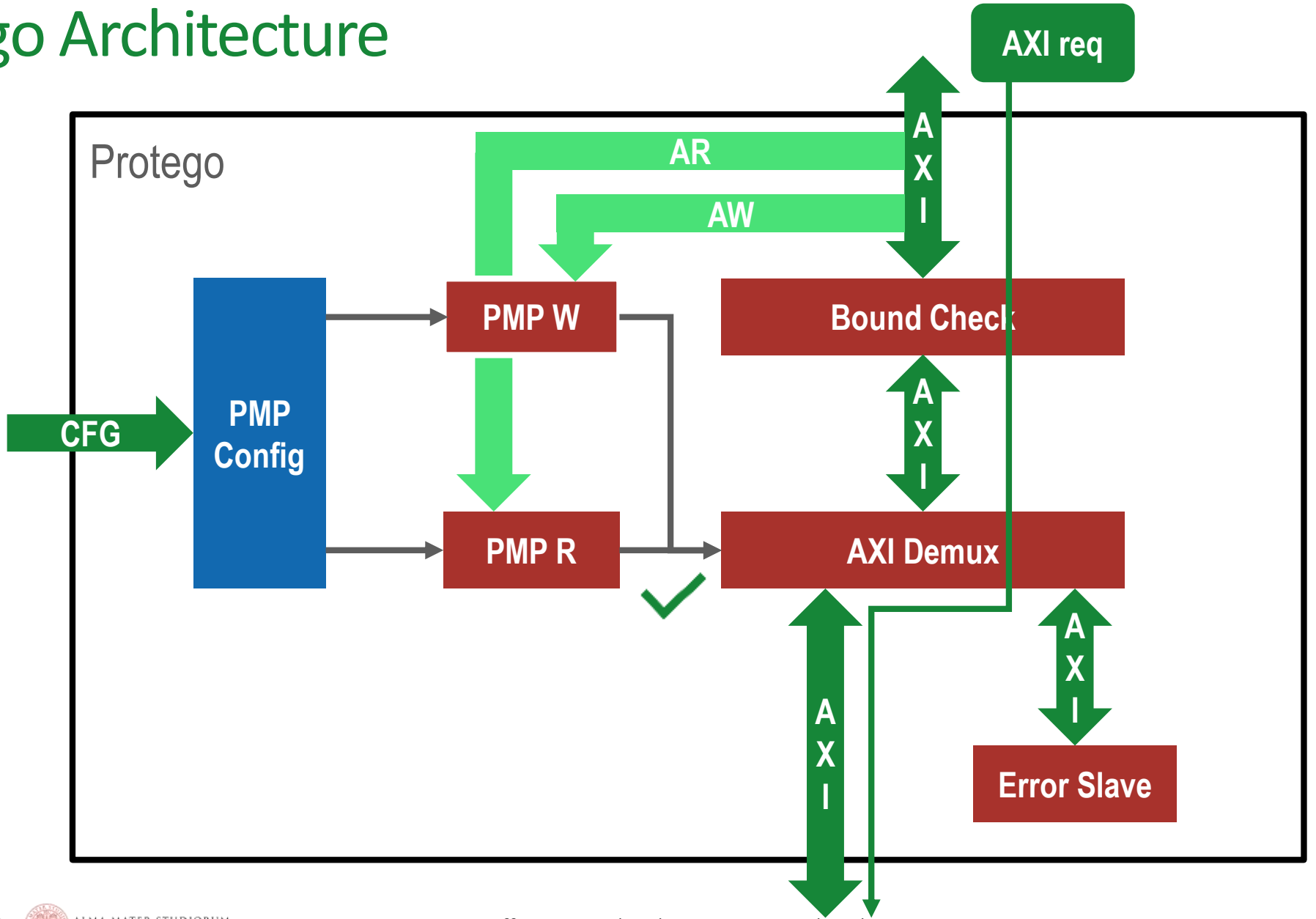
Protego Architecture



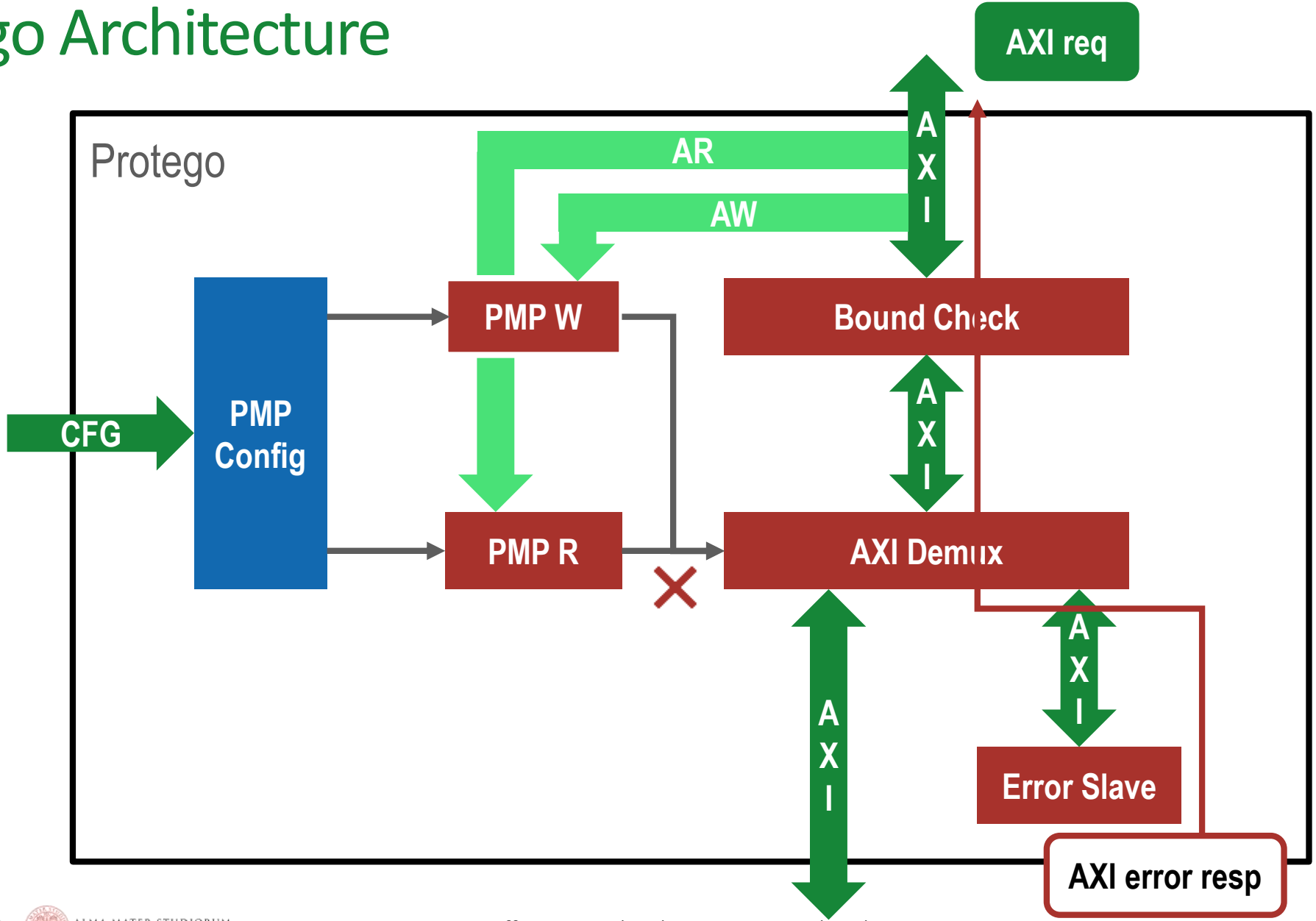
Protego Architecture



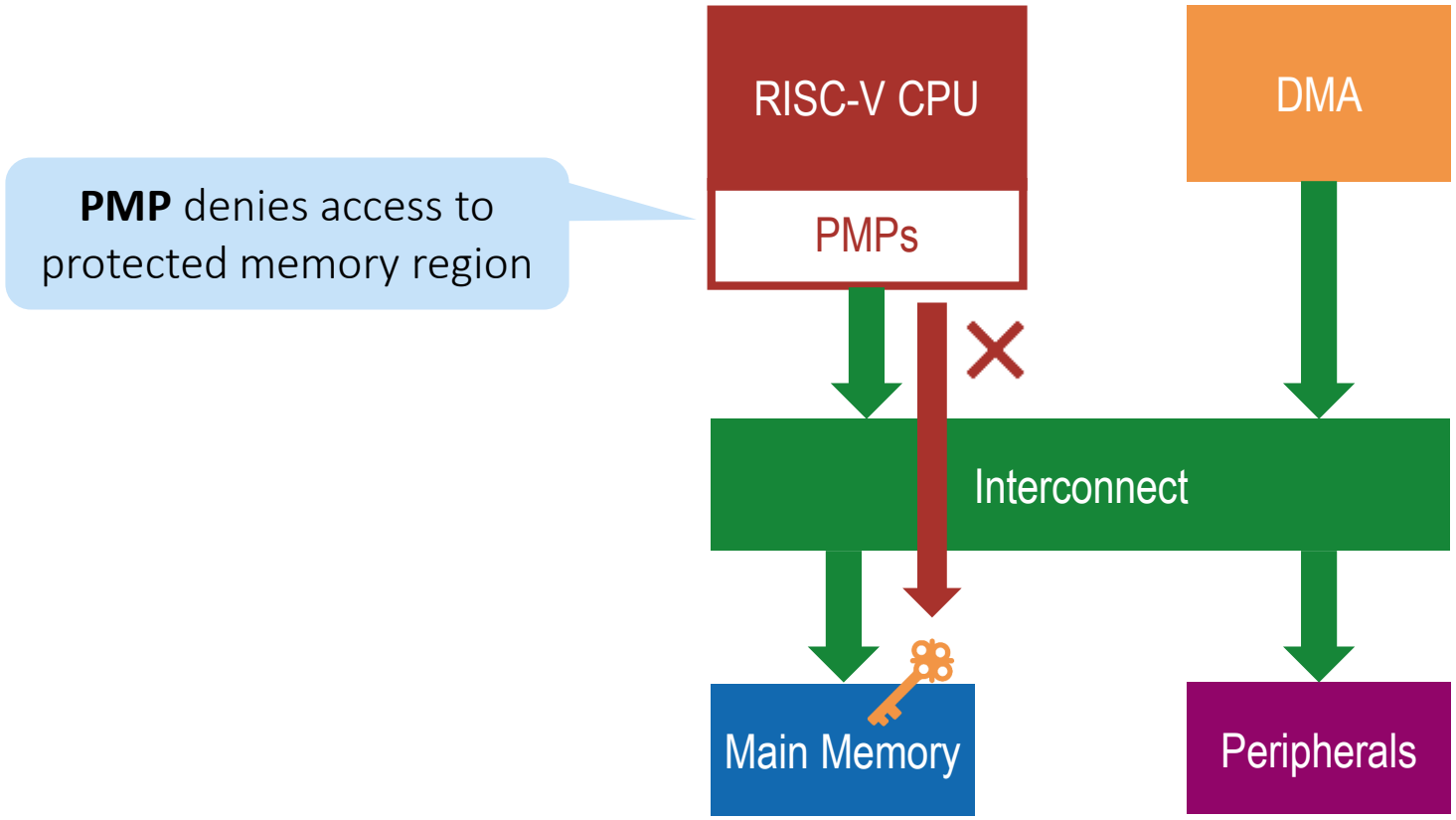
Protego Architecture



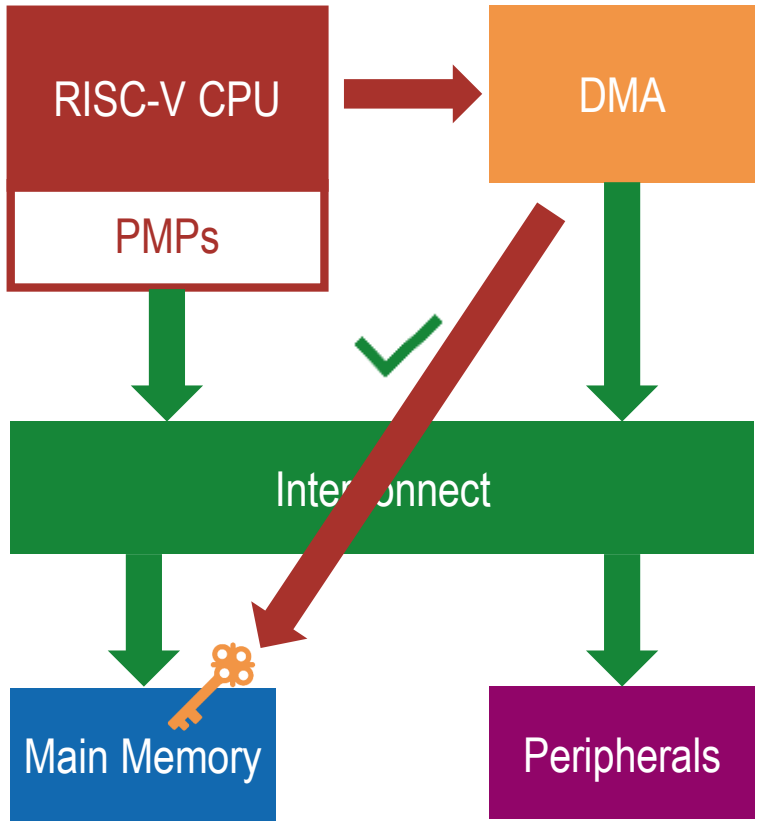
Protego Architecture



Case Study: DMA Attack

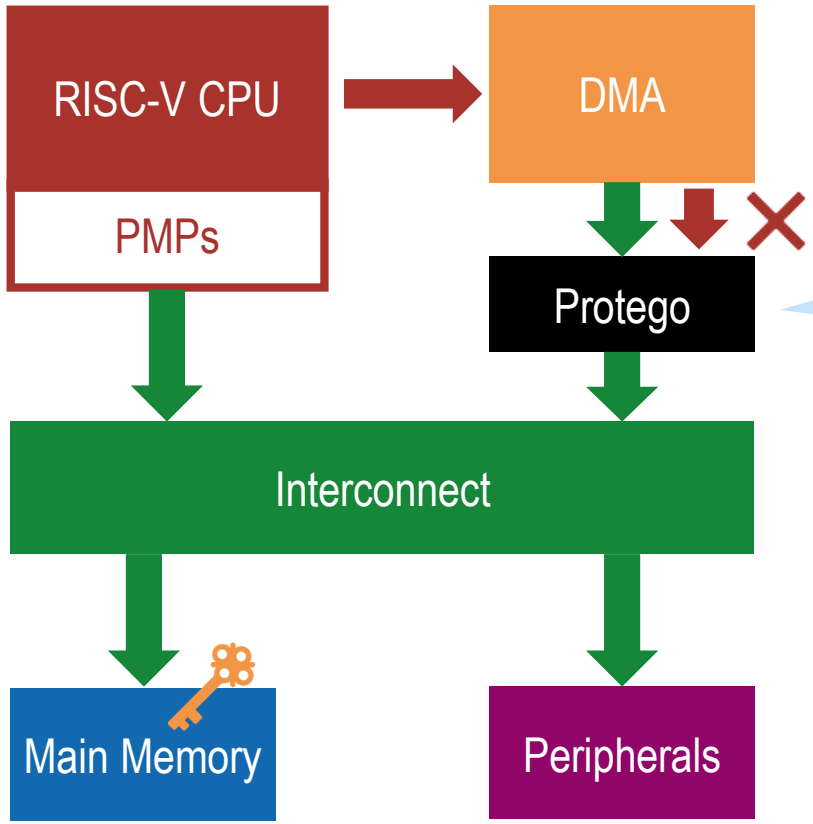


Case Study: DMA Attack



DMA can be programmed to access protected memory instead, **bypassing PMP**

Case Study: DMA Attack



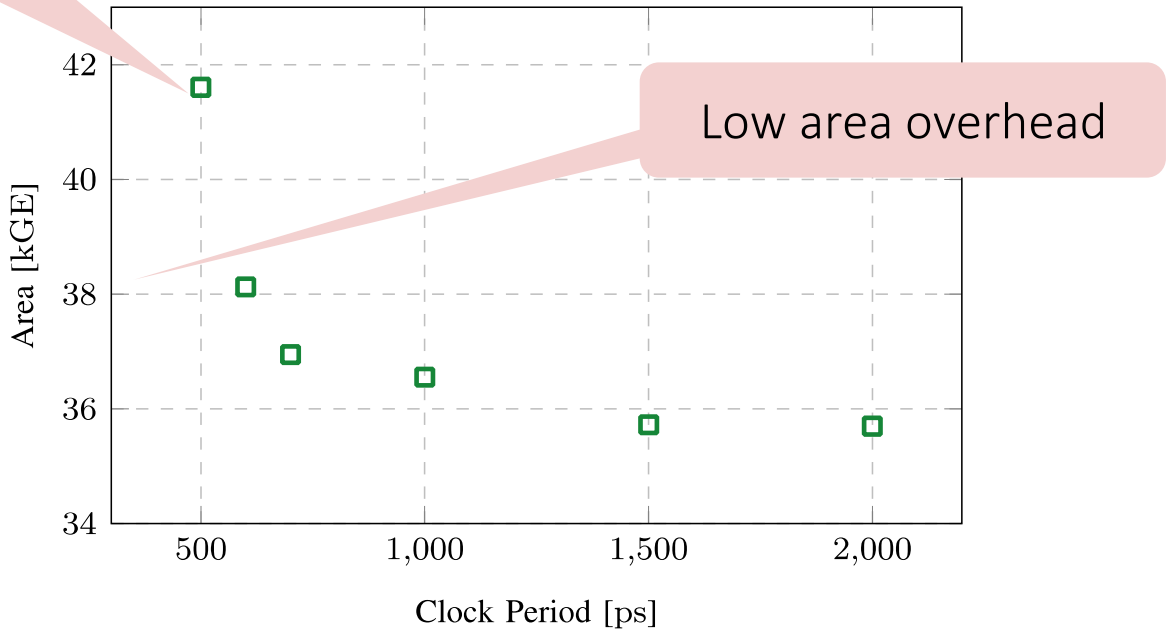
Protego **extends PMP** to heterogeneous system masters

Area vs. Timing

Reaches up to **2 GHz**

Configuration

Parameter	Value
AXI4 address width	64 bits
AXI4 data width	64 bits
AXI4 ID width	4 bits
AXI4 user width	1 bit
Inflight transactions	4
Number of IOPMP entries	16
IOPMP granularity	4 KiB

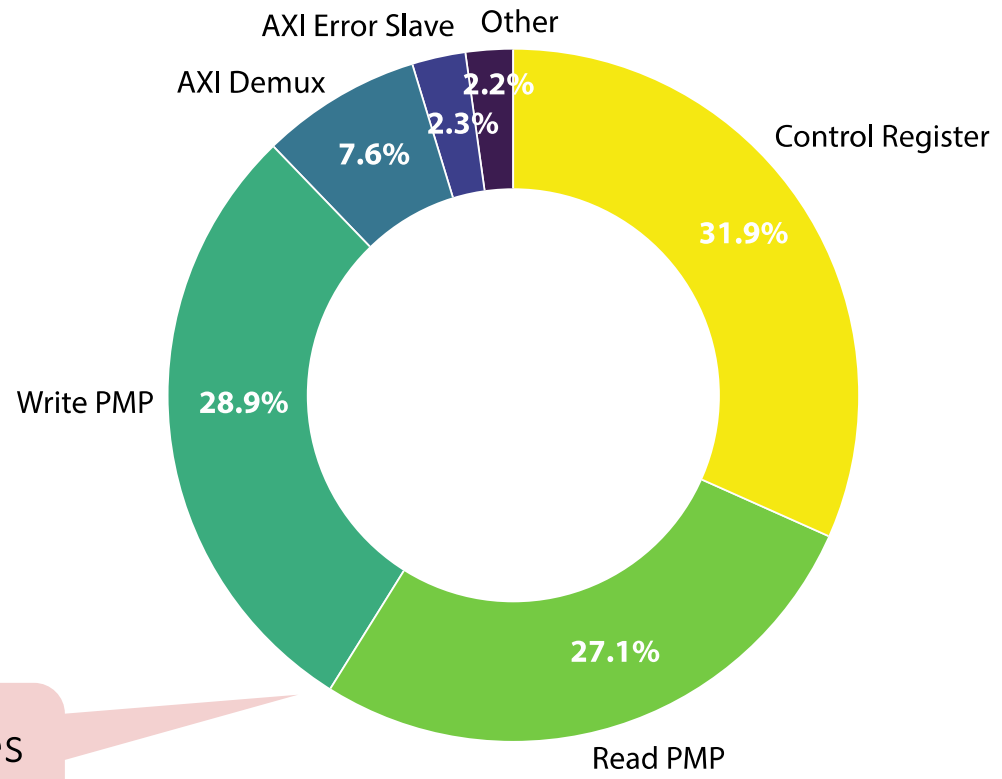


GF22FDX, 0.8V, 25° C

Area Breakdown

Configuration

Parameter	Value
AXI4 address width	64 bits
AXI4 data width	64 bits
AXI4 ID width	4 bits
AXI4 user width	1 bit
Inflight transactions	4
Number of IOPMP entries	16
IOPMP granularity	4 KiB



PMP logic consumes most area

GF22FDX, 0.8V, 25° C, 1.4 GHz

Existing IOPMP Work

- RISC-V draft specification [1]
- Few recent implementations exist
  - DITES [2]
    - 3889 LUTs, 1211 Registers
  - IOPMP [3]
    - 6 cycles, 1GHz, ca. 380 kGE
- To the best of our knowlegde, **first open-source implementation**

Work in progress

Concurrent to this work

[1] RISC-V IOPMP Task Group, IOPMP Proposal. https://github.com/riscv-admin/iopmp/blob/main/specification/IOPMP- poposal-v0-1.docx, 19-Mar.-2022

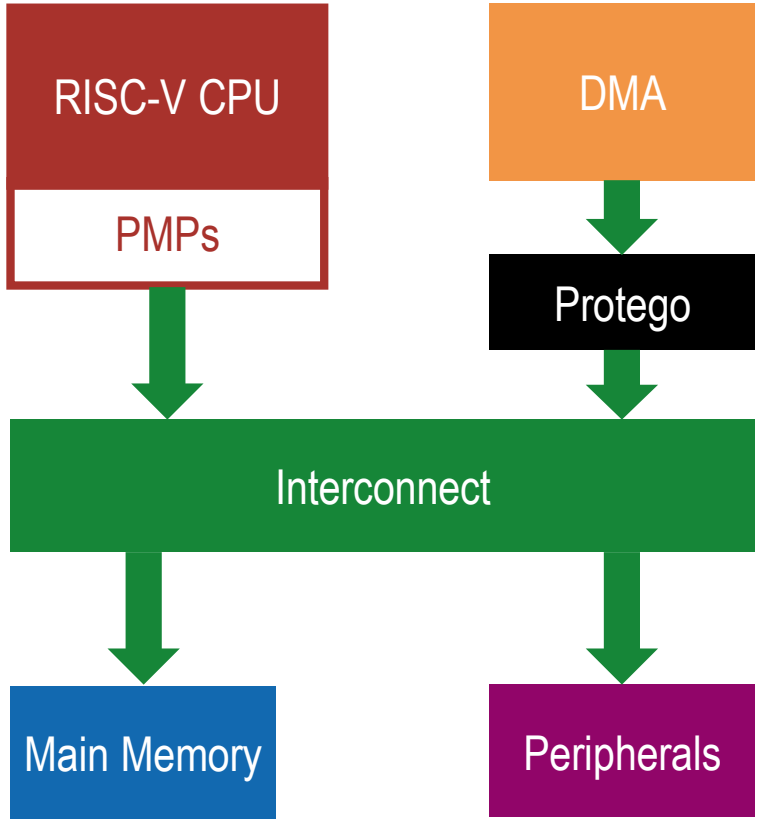
[2] Chen, Yuehai, Huarun Chen, Shaozhen Chen, Chao Han, Wujian Ye, Yijun Liu, and Huihui Zhou,"DITES: A Lightweight and Flexible Dual-Core Isolated Trusted Execution SoC Based on RISC-V" Sensors 22, 2022, no. 16: 5981 doi: 10.3390/s22165981

[3] Ng, Ang and Law, "A Realization of IO Physical Memory Protection for RISC-V Systems," 2022 IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), Penang, Malaysia, 2022, pp. 375-380, doi: 10.1109/MCSoC57363.2022.00066.

Conclusion

- **Protego**: configurable IOPMP for RISC-V
- Allows for physical memory protection in heterogeneous systems
- Ultra-low hardware overhead of ca. **40 kGE**, running at up to **2 GHz**
- Available **open source**

`github.com/pulp-platform/axi-io-pmp`



Thank you!

IOPMP Configuration

At compile-time

Parameter	Value
AXI4 address width	64 bits
AXI4 data width	64 bits
AXI4 ID width	4 bits
AXI4 user width	1 bit
Inflight transactions	4
Number of IOPMP entries	16
IOPMP granularity	4 KiB

At run-time